Homework 3

Due Date: Tuesday, November 8, 2005 **Points**: 100

1. (*25 points*) In Firday's class, I mentioned the *rsh* program. This program, and the related programs *rlogin* and *rcp*, allow a user (call her *ursula*) on one system(call it *origin*) to connect to another system (call it *destin*) without supplying a password. Basically, Ursula logs into *destin* and sets up a file, called a *.rhosts file*, that names host *origin* and user *ursula*. This tells the host *destin* that whenever *ursula* tries to log in from host *origin*, the remote host *origin* is trusted to have authenticated *ursula* properly, and no further authentication—like asking for a password—is to be done. What assumption(s) is (are) being made? When is installing these three programs a good idea, and when is it a bad idea?
2. (*20 points*) A cryptographer once stated that cryptography could provide complete security, and that any other computer security controls were unnecessary. Why is he wrong? (*Hint:* Think about using a cipher. What parts or aspects of using the cipher does the cipher itself not protect? Could you protect those aspects using a different cipher? If you could, what does *that cipher* assume?)
3. (*20 points*) Let k be the number corresponding to the encipherment key for a Caesar cipher. (So, in English, 'A' is 0, 'B' is 1, and so forth.) The decipherment key differs; it is $(26 - k) \bmod 26$. (Thus, the decipherment key corresponding to the encipherment key 'B', or 1, is $(26 - 1) \bmod 26 = 25$, or 'Z'.) One of the characteristics of a public key system is that the encipherment and decipherment keys are different. Why then is the Caesar cipher a classical cryptosystem, not a public key cryptosystem? Be specific.
4. (*10 points*) Please decipher the following Cæsar cipher: TEBKFKQEBZLROPBLCERJXKBSBKQP.
5. (*25 points*) In class, we discussed system names at the transport layer (host names), the network layer (IP addresses), and the data link layer (MAC addresses). Now consider a file system *data*. The file system is associated with the host on which it resides (call this host *reside*). But when another host (call it *remote*) is given access to that file system, users on that host refer to the file system by its name, *not* by the name of the system on which it resides.
   a. Assume that the system administrator of *remote* must first mount the file system by saying something like "give my users access to file system *data* on *reside*". Please describe how one might implement this. In other words, if a user reads a file on file system *data*, what happens?
   b. Now assume the system administrator need do nothing (no mounting required). How might one implement this; if a user reads a file on file system *data*, what happens the first time? The next time?

Extra Credit

6. (*25 points*) Solve the following Vigenère cipher: TSMVM MPPCW CZUGX HPECP RFAUE IOBQW PPIMS FXIPC TSQPK SZNUL OPACR DDPKT SLVFW ELTKR GHIZS FNIDF ARMUE NOSKR GDIPH WSGVL EDMCM SMWKP IYOJS TLVFA HPBJI RAQIW HLDGA IYOUX.